

FILED
LOGGEDENTERED
RECEIVED

AO 106 (Rev. 04/10) Application for a Search Warrant

SEP 21 2018

UNITED STATES DISTRICT COURT

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTYfor the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Google, Inc. Subject Accounts 1-3, further described in
Attachment A

Case No.

MJ18-441

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Google, Inc. Subject Accounts (1) toddsmckennon@gmail.com (2) lindsayjmckennon@gmail.com

(3) OliviaDreamLover@gmail.com, further described in Attachment A, attached hereto and incorporated herein.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1952

18 U.S.C. § 2421

18 U.S.C. § 1956

Offense Description

Interstate and foreign travel or transportation in aid of racketeering enterprises

Transportation of any individual in interstate or foreign commerce

Money Laundering

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

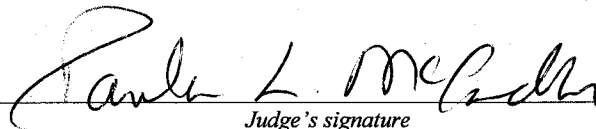
Joshua Anderson, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/21/2018

City and state: Seattle, Washington



Judge's signature

Paula L. McCandlis, United States Magistrate Judge

Printed name and title

ATTACHMENT A

GOOGLE, INC. ACCOUNTS TO BE SEARCHED

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following Google, Inc. accounts, that are stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California:

toddsckennon@gmail.com, (Subject Account #1)

lindsayjckennon@gmail.com and (Subject Account #2)

OliviaDreamLover@gmail.com (Subject Account #3)

ATTACHMENT B**I. Section I - Information to be disclosed by Google, Inc., for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., including any data, messages, records, files, logs, or information that has been deleted but is still available to Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All electronic mail content and/or preserved data (including e-mail, attachments, and embedded files);

b. All subscriber records associated with the specified account, including 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. all contact lists;

d. all Google Calendar content;

e. all Google Drive content (including backups of any apps stored on Google Drive;

f. all Google Sheets content;

g. all Google Forms content;

h. all Google Apps Script content;

i. all Google Maps content;

j. all Google Photos content;

- k. all Google Search Console content;
- l. all Google Web & Activity content;
- m. all Google Chrome Sync content;
- n. all Google Location History content;
- o. all Google Developers Console content;
- p. all Google Voice content;
- q. all Android content;
- r. all Google Alerts content;
- s. all Google Profile content, including all Google+ content;
- t. all account history, including any records of communications

between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

This Search Warrant also requires Google to produce the following information for accounts linked to the SUBJECT ACCOUNTS (collectively the "**LINKED SUBJECT ACCOUNTS**"):

- a. a list of all other Google accounts linked to the SUBJECT ACCOUNTS because of cookie overlap;
- b. a list of all other Google accounts that list the same SMS phone number as the SUBJECT ACCOUNTS;
- c. a list of all other Google accounts that list the same recovery e-mail address as the SUBJECT ACCOUNTS;
- d. and a list of all other Google accounts that shared the same creation IP address the SUBJECT ACCOUNTS within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

f. All records and other information (not including the contents of communications) relating to the Linked Subject Accounts, including:

i. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination e-mail addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the accounts to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of (a) Interstate and foreign travel or transportation in aid of racketeering enterprises in violation of 18 U.S.C § 1952; (b) Transportation for purposes of prostitution in violation of 18 U.S.C. § 2421; and (c) Money laundering in violation of 18 U.S.C. § 1956 those violations occurring between January 2017 to the

1 present, for each of the SUBJECT ACCOUNTS listed on Attachment A, and any linked
2 accounts, including the following:

3 a. Content that serves to identify any person who uses or accesses the
4 subject account or who exercises in any way any dominion or control over the account;

5 b. Content relating to planned, attempted, or successful breaches of or
6 intrusions into victims' computers or networks;

7 c. Content relating to the creation, acquisition, transfer, sharing, testing
8 or sale of malicious software;

9 d. Content related to computer programing, software operations, and
10 networking;

11 e. Content relating to the acquisition, transfer, sharing, sale, or disposal
12 of servers, e-mail accounts, or other web services accounts used by the account holder or
13 co-conspirators to facilitate computer intrusions;

14 f. Content that identifies victims of computer intrusions perpetrated by
15 the account holder or co-conspirators:

16 g. Content that constitute communications in furtherance of the crimes
17 enumerated above;

18 h. Content relating to the acquisition, transfer, distribution, sharing or
19 sale of stolen credit card, debit card, gift card, or payment card numbers;

20 i. Content that may identify assets including bank accounts,
21 commodities accounts, trading accounts, personal property and/or real estate that may
22 represent proceeds of computer intrusion activity or fraud or are traceable to such
23 proceeds;

24 j. Content that may reveal the current or past location of the individual
25 or individuals using the subject account;

26 k. Content that may reveal the identities of and relationships between
27 co-conspirators;

1 l. Content that may identify any alias names, online user names,
2 "handles" and/or "nics" of those who exercise in any way any dominion or control over
3 the specified account as well as records or information that may reveal the true identities
4 of these individuals;

5 m. Other log records, including IP address captures, associated with the
6 specified account;

7 n. Subscriber records associated with the specified account, including
8 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of
9 session times and durations; 4) length of service (including start date) and types of
10 services utilized; 5) telephone or instrument number or other subscriber number or
11 identity, including any temporarily assigned network address such as internet protocol
12 address, media access card addresses, or any other unique device identifiers recorded by
13 Google, Inc. in relation to the account; 6) account log files (login IP address, account
14 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
15 and source of payment; and 9) lists of all related accounts;

16 o. Records of communications between Google, Inc. and any person
17 purporting to be the account holder about issues relating to the account, such as technical
18 problems, billing inquiries, or complaints from other users about the specified account.
19 This to include records of contacts between the subscriber and the provider's support
20 services, as well as records of any actions taken by the provider or subscriber as a result
21 of the communications.

22 p. Android identification number, MEID, and cellular telephone
23 number

24 q. Information identifying accounts that are linked or associated with
25 the SUBJECT ACCOUNTS.

1 **AFFIDAVIT OF JOSHUA ANDERSON**

2 STATE OF WASHINGTON)
 3) ss
 4 COUNTY OF KING)

5 I, Joshua Anderson, having been duly sworn, state as follows:

6 **AFFIANT BACKGROUND**

7 1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and
 8 have been so since January 2017. I am currently assigned to an Organized Crime and
 9 Public Corruption Squad within the Seattle Division of the FBI. During my employment
 10 with the FBI, I have investigated various federal criminal violations, to include human
 11 trafficking and prostitution. I have attended the Federal Bureau of Investigation Basic
 12 Field Training Course for new Special Agents, and attended training in prostitution and
 13 human trafficking investigations at the Seattle Field Office. I have participated in
 14 multiple prostitution and human trafficking investigations, to include criminal violations
 15 of federal human trafficking-related offenses, during the course of which I have
 16 participated in physical surveillance and executions of warrants.

17 2. I am familiar with common methods of investigating human trafficking and
 18 prostitution organizations, and have become familiar with the methods of operation of
 19 human traffickers, including, but not limited to: their methods of transporting sex
 20 workers, advertising prostitution services, concealing prostitution activities, their use of
 21 cellular telephones, their use of mobile applications, their use of code words, counter-
 22 surveillance, and other methods of avoiding detection of law enforcement. I am also
 23 familiar with the various methods of concealing and laundering the proceeds of
 24 prostitution activities.

25 **EMAILS TO BE SEARCHED**

26 3. I make this Affidavit in support of an application for a Search Warrant
 27 authorizing the examination of the following email accounts (the "Subject Email
 28 Accounts"): toddsmckennon@gmail.com, lindsayjmckennon@gmail.com and

1 OliviaDreamLover@gmail.com including all subscriber and log records associated with
2 these accounts.

3 4. The domain name gmail.com is owned and operated by webhost and email
4 service provider Google, Inc. ("Google"), located at 1600 Amphitheatre Parkway,
5 Mountain View, California, 94043. The information to be searched is described in the
6 following paragraphs and in Attachment B, and is stored at a premises controlled by
7 Google.

8 5. This affidavit is made in support of an application for a search warrant
9 under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to
10 disclose to the government copies of the information (including the content of
11 communications) further described in Section I of Attachment B. Upon receipt of the
12 information described in Section I of Attachment B, government-authorized persons will
13 review that information to locate the items described in Section II of Attachment B.

14 **SCOPE OF AFFIDAVIT**

15 6. The facts set forth in this Affidavit are based on my own personal
16 knowledge; knowledge obtained from other individuals during my participation in this
17 investigation, including other law enforcement officers; review of documents and records
18 related to this investigation; communications with others who have personal knowledge
19 of the events and circumstances described herein; and information gained through my
20 training and experience. Because this Affidavit is submitted for the limited purpose of
21 establishing probable cause in support of the Application for a Search Warrant, it does
22 not set forth each and every fact that I, or others, have learned during the course of this
23 investigation but rather those relevant to the question of whether probable cause exists to
24 issue the requested search warrant.

25 **THE INVESTIGATION**

26 7. In August of 2017, a woman named L.M. contacted the Federal Bureau of
27 Investigation (FBI) in Seattle, Washington, and provided information about her pimp,
28

1 Todd McKennon. L.M. explained that McKennon had recently assaulted her and that she
2 was fearful of him.

3 8. During this interview L.M. stated that she met McKennon after responding
4 to an advertisement on Craigslist about becoming a model. However, when L.M. met
5 McKennon, instead discussing opportunities in modeling, McKennon recruited her to
6 become a sex worker for him.

7 9. In early 2017, L.M. began working for McKennon. L.M. stated that
8 McKennon had her post prostitution advertisements on various internet web sites.
9 McKennon would rent hotel rooms at local hotels where L.M. would meet the
10 prostitution customers. She said that some of the hotels McKennon used were the
11 Residence Inn by Marriott Bellevue, Courtyard by Marriott Kirkland, Hyatt Regency
12 Bellevue, Hyatt House Bellevue and Hyatt House Redmond.

13 10. L.M. also stated that on one occasion, McKennon had her fly to Hawaii and
14 engage in prostitution with a high-paying customer for approximately one week.¹

15 11. L.M. stated McKennon would split the prostitution proceeds with her.²
16 McKennon would have L.M. deposit his share of the proceeds into his bank account by
17 utilizing a debit card.

18 12. After a period of time, L.M. stated that she and McKennon became
19 romantically involved and she began living with him. L.M. believed, based on what she
20 learned from McKennon, that he has been involved in prostitution for approximately two
21 decades. According to L.M., McKennon was known as "Mr. Kirkland" and that he had
22 several sex workers consistently working for him in Kirkland, Bellevue, Redmond, and
23 Seattle. L.M. also stated that McKennon had supported himself for years through
24 prostitution.

25
26 ¹¹ I located an advertisement posted by L.M. that stated that she had recently returned from Hawaii but further
details were not provided.

27 ² Initially, McKennon allowed L.M. to keep 60% of the proceeds but later reduced it to 50%.

1 13. L.M. believed that McKennon would also occasionally facilitate and
2 arrange for out of state prostitution activities. In approximately May 2017, McKennon
3 sent her to Hawaii to work for five days with one customer.

4 14. During the August 2017 interview, L.M. indicated that she was fearful of
5 McKennon and expressed a desire to get away from him. The FBI assisted L.M. in flying
6 to Alaska, where she was from, as a way to protect her. The FBI lost contact with L.M.
7 after she returned to Alaska. A short time later, the FBI learned of L.M. was back in
8 Washington working for McKennon again. L.M. and McKennon appear to be
9 romantically involved at this point and they also live together.

10 15. In checking McKennon's background, I learned that in 2013 McKennon
11 was investigated by the Kirkland Police Department for promoting prostitution. I
12 received and reviewed Kirkland Police report WA017080. In that report, a concerned
13 citizen contacted the Kirkland Police Department to complain about suspicious activity
14 occurring at neighboring townhouse in the Springtree Condos. The complainant stated
15 that he/she and other neighbors had observed what they believed to be prostitution
16 activity occurring at the townhouse located at 11408 105th Place NE, Kirkland,
17 Washington. The complainant explained that they noticed males in high priced cars park
18 nearby and enter the residence. The males stayed for exactly one hour and would then
19 leave. Within 10 minutes of the men leaving the neighbors would see a woman leaving
20 the residence in a taxi. Within 30 minutes of the woman leaving, a black GMC Yukon
21 arrived backed up to the garage. The driver of the Yukon (later identified as Todd
22 McKennon) would collect the garbage bags, and often a white envelope, then leave.

23 16. The activity stopped when the owner of the condo sold it. The owner of the
24 condominium has been identified as Shelly Straw who is Todd McKennon's former
25 girlfriend and mother of his child. It appears that McKennon was never charged with
26 promoting prostitution or any other criminal activity arising out of that investigation.

27 17. Based on the information provided by L.M. the FBI and local authorities
28 began parallel investigations of Todd McKennon's sexual trafficking activities.

1 18. As part of that investigation, local law enforcement officers obtained a state
2 issued search warrant for the internet classified advertising site, TNA Board, for L.M.'s
3 advertisements. TNA Board is an online site that is used for advertising sexual services
4 such as commercial sex acts. In reviewing the information provided by TNA Board,
5 agents found an advertisement, posted on March 20, 2018, for L.M. under pseudonym
6 "Olivia Heart." In this advertisement, L.M. is offering sex services for \$500/hour in the
7 Seattle, Bellevue, Kirkland and Redmond areas. The advertisement has graphic, sexually
8 explicit photos of L.M. In the advertisement L.M. says "Come play and misbehave with
9 me! Your ultimate pleasure provider!" Further stating, "Your wish is my command,
10 come and spend some naughty time with me!"

11 19. The state law enforcement also obtained a state search warrant for L.M.'s
12 advertisements on another online advertising site called CityVibe. In reviewing the
13 information provided by CityVibe, law enforcement officers found an advertisement for
14 L.M. posted on February 19, 2018. In this advertisement, L.M., using her pseudonym
15 "Olivia Heart," is offering sex services for \$500/hour under in the Monterey, San Jose
16 area of California. The advertisement contains graphic, sexually explicit photos of L.M.
17 This advertisement states that L.M. "loves to please a man in whichever way he wants to
18 be pleased." It further states, "I have a pretty good knack of finding out your turn
19 ons...And I will be sure you know my turn ons." L.M.'s advertisement goes on to claim
20 she is, "[v]ery open minded and would love to share with you my exclusive "SND" gift
21 (sexy, naughty, dirty) for \$500/hour." Finally it states, "I promise you will not be
22 disappointed."

23 20. As part of the investigation, myself, as well as other FBI agents have
24 obtained bank records. Based on the records we learned that McKennon was renting
25 rooms at the Hyatt Regency Hotel in Bellevue, the Residence Inn by Marriott Seattle
26 Bellevue in Bellevue, the Hyatt House in Redmond, and the Courtyard by Marriott
27 Seattle Kirkland in Kirkland, Washington. We then subpoenaed booking records from
28 those hotels and learned that McKennon was booking rooms at these hotels frequently.

21. According to the general manager at the Residence Inn Marriott in Bellevue, McKennon has an elite membership with their national hotel chain in which he maintains through reserving rooms for a minimum of 60 nights per year. Furthermore, according to the general manager at the Hyatt House in Redmond and Bellevue, McKennon has an elite membership as a "Globalist" with the Hyatt Hotel brand that is earned by reserving rooms for a minimum of 55 nights per year. On multiple occasions, McKennon reserves rooms at the Hyatt Regency in Bellevue utilizing the "Triple A" discount rate in which he is upgraded to a suite. Furthermore, the "Globalist" status allows for early check-in, which surveillance has observed, as well as for later than normal checkout. On one instance, surveillance observed individuals departing the hotel room after 4pm and McKennon was not charged for that night.

22. Myself and other law enforcement agents have conducted six surveillances in the past three months at various locations and have had a chance to observe the operation criminal enterprise. These locations include:

- Residence Inn by Marriott Seattle Bellevue on January 31, 2018, February 26, 2018, and March 23, 2018, located at 14455 NE 29th Place, Bellevue, Washington,
- Courtyard by Marriott Seattle/ Kirkland located at 11215 NE 124th Street, Kirkland, Washington, on January 31, 2018 and April 13, 2018;
- Hyatt House Seattle Redmond located at 15785 Bear Creek Parkway, Redmond, Washington, on May 17, 2018 and May 18, 2018.

23. The surveillance teams observed McKennon on the premises of all of these hotels, typically checking in and then either dropping L.M. off or picking L.M. up. At no point during surveillance was McKennon observed staying in a hotel room for which he had a reservation.

24. Over the course of these surveillances, L.M. and another female, later identified as D.H.S., who was identified based on Washington State Driver's License information obtained during surveillance, are the predominant sex workers. D.H.S. was

1 identified after arriving at a known hotel, entering the hotel room that McKennon had
2 reserved, working for a couple hours and then departing in her registered vehicle. Both
3 L.M. and D.H.S. have been positively identified entering the rooms being used by
4 McKennon while McKennon is not at the hotel. D.H.S. and L.M. are very discrete when
5 entering or exiting the hotels. They have not been seen stopping at the front desk to
6 obtain a key for access to the room. They have been seen parking in hotel back lots,
7 using the side entrances of the hotels and using the stairs as opposed to using the main
8 entrance and the elevator at multiple hotel properties.

9 25. During the surveillances multiple men have been observed exhibiting
10 behaviors consistent with being sex customers. After arriving at the parking in a lot and
11 the customers have been observed waiting in their car. Based on my experience the
12 customers wait in the car until they receive a text message informing the customer which
13 room to go to. The men do not stop at the front desk to obtain a room key or to obtain
14 directions to the rooms. These customers stay in the room for approximately one hour
15 which is the time period noted in the escort ads.

16 26. During a surveillance at the Hyatt Regency in Bellevue on June 29, 2018,
17 L.M. and McKennon were observed arriving to the hotel room together. McKennon and
18 L.M. left for a short period of time and L.M. returned alone. A few minutes later, a male
19 customer entered the room. After approximately one hour, the male customer departed.
20 A few minutes later, McKennon re-entered the room and he and L.M. departed together,
21 proceeding to Daniel's Broiler for drinks and dinner.

22 27. McKennon's behavior is consistent with someone who is running a
23 criminal sex organization. He has been observed arriving at hotels on the day of check-in
24 to pick up keys, drop off and pick up L.M. for appointments.

25 28. I obtained McKennon's bank account records for Bank of America, account
26 number xxxxxxxx3034, via grand jury subpoena. Based on these records, for the period
27 between 2016 to the present date over \$500,000 has been deposited into this Account.
28 The FBI has verified that approximately \$330,000 as being cash deposits. Records

1 obtained from the Bank of America of account ending in 3034, show that many of the
2 cash deposits are made through an automated teller machine or at the counter. The bank
3 records the FBI has obtained shows McKennon, L.M., and D.H.S. making cash deposits
4 into the 3034 account. For example in a two week period, the records show that \$11,000
5 in cash was deposited into the account. The records show that McKennon will
6 subsequently use the funds from this account to pay for hotel rooms and online
7 advertisements.

8 29. Since 2012 according to the Washington State Employment Security
9 Department McKennon has reported no wages.

10 30. In the 2017 interview, L.M. disclosed that she and McKennon used a
11 suitcase which had sex supplies and garbage bags for cleaning up. During the
12 surveillance, both L.M. and D.H.S. have been observed with a roller bag while entering
13 the hotel. On one occasion D.H.S. was observed arriving at a hotel, carrying multiple
14 bags to include the roller bag while entering the hotel room. Later, D.H.S. travelled to
15 McKennon's residence where she stayed for approximately two hours before returning to
16 the hotel where a male visited her hotel room.

17 31. The investigation has developed evidence that
18 toddsmckennon@gmail.com, lindsayjmckennon@gmail.com and
19 oliviadreamlover@gmail.com are being used in connection with the criminal scheme.
20 McKennon is utilizing the email toddsmckennon@gmail.com and
21 lindsayjmckennon@gmail.com for any correspondence with hotels in furtherance of his
22 criminal prostitution enterprise. As recently as June 2018, L.M. is utilizing
23 oliviadreamlover@gmail.com to post advertisements in furtherance of prostitution
24 activities.

25 **BACKGROUND REGARDING INFORMATION TECHNOLOGY**

26 32. Google is an email service provider. Email service providers provide their
27 clients/subscribers with a dedicated email domain name and space on their servers for the
28 storage of client emails and associated files. Therefore, the computers of Google are

1 likely to contain stored electronic communications (including retrieved and un-retrieved
2 email for Gmail users) and information concerning clients/subscribers and their use of
3 Google email services, respectively, such as account access information, email
4 transaction information, and account application information.

5 33. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1),
6 and includes an electronic, magnetic, optical, electrochemical, or other high speed data
7 processing device performing logical, arithmetic, or storage functions, and includes any
8 data storage facility or communications facility directly related to or operating in
9 conjunction with such device.

10 34. As explained herein, information stored in connection with an e-mail
11 account may provide crucial evidence of the "who, what, why, when, where, and how" of
12 the criminal conduct under investigation, thus enabling the United States to establish and
13 prove each element or alternatively, to exclude the innocent from further suspicion. In my
14 training and experience, the information stored in connection with an e-mail account can
15 indicate who has used or controlled the account. This "user attribution" evidence is
16 analogous to the search for "indicia of occupancy" while executing a search warrant at a
17 residence. For example, e-mail communications, contacts lists, and images sent (and the
18 data associated with the foregoing, such as date and time) may indicate who used or
19 controlled the account at a relevant time.

20 35. Further, information maintained by the e-mail provider can show how and
21 when the account was accessed or used. For example, as described below, e-mail
22 providers typically log the Internet Protocol ("IP") addresses from which users access the
23 email account along with the time and date. By determining the physical location
24 associated with the logged IP addresses, investigators can understand the chronological
25 and geographic context of the e-mail account access and use relating to the crime under
26 investigation. This geographic and timeline information may tend to either inculcate or
27 exculpate the account owner. Additionally, information stored at the user's account may
28 further indicate the geographic location of the account user at a particular time (e.g.,

1 location information integrated into an image or video sent via email). Lastly, stored
2 electronic data may provide relevant insight into the e-mail account owner's state of mind
3 as it relates to the offense under investigation. For example, information in the e-mail
4 account may indicate the owner's motive and intent to commit a crime (e.g.,
5 communications relating to the crime), or consciousness of guilt (e.g., deleting
6 communications in an effort to conceal them from law enforcement). Based on my
7 training, experience and knowledge, I know the following: the internet is a global system
8 of interconnected computer networks that use the standard Internet Protocol Suite
9 (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of
10 millions of private, public, academic, business, and government networks, of local to
11 global scope, that are linked by a broad array of electronic, wireless and optical
12 networking technologies. The internet can also be defined as a worldwide
13 interconnection of computers and computer networks that facilitate the sharing or
14 exchange of information among users. The internet carries a vast range of information
15 resources and services, such as the inter-linked hypertext documents of the World Wide
16 Web (WWW) and the infrastructure to support electronic mail.

17 36. E-mail is a popular form of transmitting messages and files in an electronic
18 environment between computer users. When an individual computer user sends an e-
19 mail message, it is initiated at the user's computer, transmitted to the subscriber's mail
20 server, and then transmitted to its final destination. A server is a computer that is
21 attached to a dedicated network and serves many users. An e-mail server may allow
22 users to post and read messages and to communicate via electronic means.

23 37. E-mail providers generally ask their subscribers to provide certain personal
24 identifying information when registering for an e-mail account. Such information can
25 include the subscriber's full name, physical address, telephone numbers and other
26 identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of
27 payment (including any credit or bank account number). In my training and experience,
28 such information may constitute evidence of the crimes under investigation because the

1 information can be used to identify the account's user or users. Based on my training and
2 my experience, I know that even if subscribers insert false information to conceal their
3 identity, this information often provide clues to their identity, location or illicit activities.

4 38. E-mail providers typically retain certain transactional information about the
5 creation and use of each account on their systems. This information can include the date
6 on which the account was created, the length of service, records of log-in (i.e., session)
7 times and durations, the types of service(s) utilized, the status of the account (including
8 whether the account is inactive or closed), the methods used to connect to the account
9 (such as logging into the account via the provider's website), and other log files that
10 reflect usage of the account. In addition, e-mail providers often have records of the
11 Internet Protocol address ("IP address") used to register the account and the IP addresses
12 associated with particular logins to the account. Because every device that connects to
13 the Internet must use an IP address, IP address information can help to identify which
14 computers or other devices were used to access the e-mail account.

15 39. In some cases, e-mail account users will communicate directly with an e-
16 mail service provider about issues relating to the account, such as technical problems,
17 billing inquiries, or complaints from other users. E-mail providers typically retain
18 records about such communications, including records of contacts between the user and
19 the provider's support services, as well records of any actions taken by the provider or
20 user as a result of the communications. In my training and experience, such information
21 may constitute evidence of the crimes under investigation because the information can be
22 used to identify the account's user or users.

23 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

24 40. Pursuant to Title 18, United States Code, Section 2703(g), this application
25 and affidavit for a search warrant seeks authorization to permit Google and their agents
26 and employees, to assist agents in the execution of this warrant. Once issued, the search
27 warrant will be presented to Google, with direction that the companies should identify the
28

1 e-mail account described in Attachment A as well as other subscriber and log records
2 associated with the account, as set forth in Section I of Attachment B to this Affidavit.

3 41. The search warrant will direct Google to create an exact copy of the
4 specified count and records.

5 42. All forensic analysis of the data will employ only those search protocols
6 and methodologies reasonably designed to identify and seize the items identified in
7 Section II of Attachment B to the warrant. Based on my experience and training, and the
8 experience and training of other agents with whom I have communicated, it is necessary
9 to review and seize a variety of e-mail communications, chat logs and documents, that
10 identify any users of the subject account and e-mails sent or received in temporal
11 proximity to incriminating e-mails that provide context to the incriminating
12 communications.

13 **REQUEST FOR NONDISCLOSURE AND SEALING**

14 43. The government requests, pursuant to the preclusion of notice provisions of
15 Title 18, United States Code Sections 2421 and 1956; that Google, Inc. be ordered not to
16 notify any person (including the subscriber or customer to which the materials relate) of
17 the existence of this warrant for such period as the Court deems appropriate. The
18 government submits that such an order is justified because notification of the existence of
19 this Order would seriously jeopardize the ongoing investigation. Such a disclosure would
20 give the subscriber an opportunity to destroy evidence, change patterns of behavior,
21 notify confederates, or flee or continue his flight from prosecution.

22 44. It is further respectfully requested that this Court issue an order sealing,
23 until further order of the Court, all papers submitted in support of this application,
24 including the application and search warrant. I believe that sealing this document is
25 necessary because the records relate to an ongoing investigation that includes both United
26 States and foreign targets. Premature notice of investigation to any subject may
27 jeopardize investigation.
28

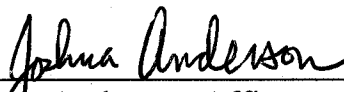
1 **CONCLUSION**

2 45. Based on the forgoing, I respectfully submit that there is probable cause
3 that the SUBJECT EMAIL ACCOUNTS contain evidence, fruits, and instrumentalities
4 of the following federal offenses: (a) Interstate and foreign travel or transportation in aid
5 of racketeering enterprises in violation of 18 U.S.C. § 1952; (b) Transportation for
6 purposes of prostitution in violation of 18 U.S.C. § 2421; and (c) Money laundering in
7 violation of 18 U.S.C. § 1956. I therefore request that the Court issue the proposed
8 Search Warrant. Because the Search Warrant will be served on Google, Inc., who will
9 then compile the requested records at a time convenient to it, reasonable cause exists to
10 permit the execution of the requested Search Warrant at any time in the day or night.

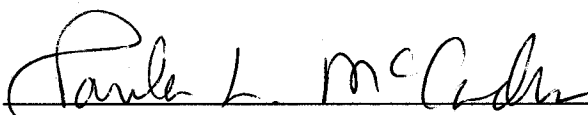
11 46. This Court has jurisdiction to issue the requested warrant because it is "a
12 court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),
13 (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . .
14 that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).
15 Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not
16 required for the service or execution of this warrant.

17 I declare under penalty of perjury that the statements above are true and correct to
18 the best of my knowledge and belief.

19 DATED this 21st day of September, 2018.

20
21 
22 Joshua Anderson, Affiant
23 Special Agent
24 Federal Bureau of Investigation

25 SUBSCRIBED AND SWORN before me this 21st day of September, 2018.

26
27 
28 THE HONORABLE PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

GOOGLE, INC. ACCOUNTS TO BE SEARCHED

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following Google, Inc. accounts, that are stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California:

toddsmckennon@gmail.com, (Subject Account #1)

lindsayjmckennon@gmail.com and (Subject Account #2)

OliviaDreamLover@gmail.com (Subject Account #3)

ATTACHMENT B**I. Section I - Information to be disclosed by Google, Inc., for search:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., including any data, messages, records, files, logs, or information that has been deleted but is still available to Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All electronic mail content and/or preserved data (including e-mail, attachments, and embedded files);

b. All subscriber records associated with the specified account, including 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. all contact lists;

d. all Google Calendar content;

e. all Google Drive content (including backups of any apps stored on Google Drive;

f. all Google Sheets content;

g. all Google Forms content;

h. all Google Apps Script content;

i. all Google Maps content;

j. all Google Photos content;

- k. all Google Search Console content;
- l. all Google Web & Activity content;
- m. all Google Chrome Sync content;
- n. all Google Location History content;
- o. all Google Developers Console content;
- p. all Google Voice content;
- q. all Android content;
- r. all Google Alerts content;
- s. all Google Profile content, including all Google+ content;
- t. all account history, including any records of communications

between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

This Search Warrant also requires Google to produce the following information for accounts linked to the SUBJECT ACCOUNTS (collectively the "**LINKED SUBJECT ACCOUNTS**"):

- a. a list of all other Google accounts linked to the SUBJECT ACCOUNTS because of cookie overlap;
- b. a list of all other Google accounts that list the same SMS phone number as the SUBJECT ACCOUNTS;
- c. a list of all other Google accounts that list the same recovery e-mail address as the SUBJECT ACCOUNTS;
- d. and a list of all other Google accounts that shared the same creation IP address the SUBJECT ACCOUNTS within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

f. All records and other information (not including the contents of communications) relating to the Linked Subject Accounts, including:

i. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination e-mail addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the accounts to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of (a) Interstate and foreign travel or transportation in aid of racketeering enterprises in violation of 18 U.S.C § 1952; (b) Transportation for purposes of prostitution in violation of 18 U.S.C. § 2421; and (c) Money laundering in violation of 18 U.S.C. § 1956 those violations occurring between January 2017 to the

1 present, for each of the SUBJECT ACCOUNTS listed on Attachment A, and any linked
2 accounts, including the following:

3 a. Content that serves to identify any person who uses or accesses the
4 subject account or who exercises in any way any dominion or control over the account;

5 b. Content relating to planned, attempted, or successful breaches of or
6 intrusions into victims' computers or networks;

7 c. Content relating to the creation, acquisition, transfer, sharing, testing
8 or sale of malicious software;

9 d. Content related to computer programing, software operations, and
10 networking;

11 e. Content relating to the acquisition, transfer, sharing, sale, or disposal
12 of servers, e-mail accounts, or other web services accounts used by the account holder or
13 co-conspirators to facilitate computer intrusions;

14 f. Content that identifies victims of computer intrusions perpetrated by
15 the account holder or co-conspirators:

16 g. Content that constitute communications in furtherance of the crimes
17 enumerated above;

18 h. Content relating to the acquisition, transfer, distribution, sharing or
19 sale of stolen credit card, debit card, gift card, or payment card numbers;

20 i. Content that may identify assets including bank accounts,
21 commodities accounts, trading accounts, personal property and/or real estate that may
22 represent proceeds of computer intrusion activity or fraud or are traceable to such
23 proceeds;

24 j. Content that may reveal the current or past location of the individual
25 or individuals using the subject account;

26 k. Content that may reveal the identities of and relationships between
27 co-conspirators;

1 l. Content that may identify any alias names, online user names,
2 “handles” and/or “nics” of those who exercise in any way any dominion or control over
3 the specified account as well as records or information that may reveal the true identities
4 of these individuals;

5 m. Other log records, including IP address captures, associated with the
6 specified account;

7 n. Subscriber records associated with the specified account, including
8 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of
9 session times and durations; 4) length of service (including start date) and types of
10 services utilized; 5) telephone or instrument number or other subscriber number or
11 identity, Including any temporarily assigned network address such as internet protocol
12 address, media access card addresses, or any other unique device identifiers recorded by
13 Google, Inc. in relation to the account; 6) account log files (login IP address, account
14 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
15 and source of payment; and 9) lists of all related accounts;

16 o. Records of communications between Google, Inc. and any person
17 purporting to be the account holder about issues relating to the account, such as technical
18 problems, billing inquiries, or complaints from other users about the specified account.
19 This to include records of contacts between the subscriber and the provider’s support
20 services, as well as records of any actions taken by the provider or subscriber as a result
21 of the communications.

22 p. Android identification number, MEID, and cellular telephone
23 number

24 q. Information identifying accounts that are linked or associated with
25 the SUBJECT ACCOUNTS.